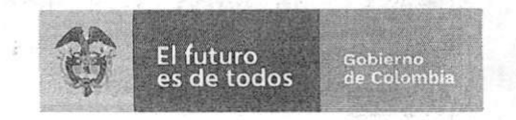


Instituto Colombiano de Bienestar Familiar
Cecilia De la Fuente de Lleras
Dirección General



RESOLUCIÓN No 4286 27 JUL 2020

Por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información, y se deroga la Resolución 9674 de 2018

LA DIRECTORA GENERAL DEL INSTITUTO COLOMBIANO DE BIENESTAR FAMILIAR CECILIA DE LA FUENTE DE LLERAS

En uso de sus facultades legales y estatutarias señaladas en las Leyes 7ª de 1979, 87 de 1993, el artículo 78 de la Ley 489 de 1998 y el artículo 2.2.9.1.3.2 del Decreto 1078 de 2015, modificado por el Decreto 1008 de 2018, y

CONSIDERANDO:

Que la Constitución Política de Colombia en el artículo 15, consagra que todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, debiendo el Estado respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas.

Que así mismo, el artículo 209 Superior establece que la administración pública, en todos sus órdenes, tendrá un control interno, el cual se ejercerá en los términos que señale la ley. Así mismo, en el artículo 269 ordena a las autoridades de las entidades públicas la obligación de diseñar y aplicar, según la naturaleza de sus funciones, métodos y procedimientos de control interno.

Que el Decreto 1078 de 2015 modificado por el Decreto 1008 de 2018, en el artículo 2.2.9.1.1.3. define a la seguridad de la información como un principio de la Política de Gobierno Digital; de igual manera, en el artículo 2.2.9.1.2.1 define la estructura de los Elementos de la Política de Gobierno Digital a través de componentes y habilitadores transversales los cuales son los elementos fundamentales de Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, que permiten el desarrollo de los anteriores componentes y el logro de los propósitos de la Política de Gobierno Digital.

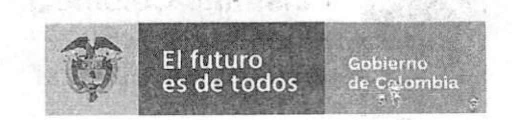
Que a través de la Resolución No. 10806 del 11 de diciembre de 2015, el ICBF adoptó la Política de Seguridad de la Información, conforme lo dispuesto en el Decreto 1078 de 2015 y en consonancia con las normas de protección de datos personales contenidas en la Ley 1581 de 2012, las normas de transparencia y acceso a la información de la Ley 1712 de 2014, así como en aquellas que las reglamentan.

Que mediante la Resolución No. 9364 de 2016, el ICBF actualizó la Política de Seguridad de la Información y definió lineamientos frente su uso y manejo, teniendo en cuenta la normativa vigente de protección de datos personales, así como de transparencia y acceso a la información, siendo modificada posteriormente por la Resolución No. 3600 del 22 de mayo de 2017.

Que mediante la Resolución No. 9674 de 2018, el ICBF actualizó la Política de Seguridad de la Información y lineamientos frente su uso y manejo, teniendo en cuenta la normativa vigente de protección de datos personales, así como de transparencia y acceso a la información.

Que en el CONPES 3854 de 2016 se establece la Política Nacional de Seguridad Digital en la República de Colombia.





RESOLUCIÓN No. - - 4286 27 JUL 2020

Por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información, y se deroga la Resolución 9674 de 2018

Que el Decreto 1499 de 2017, el cual modificó el Decreto 1083 de 2015 (Decreto Único Reglamentario del Sector de Función Pública), adoptó el Modelo Integrado de Planeación y Gestión - MIPG, definiéndolo en su artículo 2.2.22.3.2 como *"…es un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos, con el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos, con integridad y calidad en el servicio"*.

Que el artículo 2.2.22.2.1 del Decreto 1083 de 2015, sustituido por el artículo 1º del Decreto 1499 de 2017, regula las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de *"11. Gobierno Digital, antes Gobierno en Línea"* y *"12. Seguridad Digital"*.

Que mediante la Resolución No. 8080 de 2016 se aprueba el Manual del Sistema Integrado de Gestión en el ICBF, el cual cuenta con una Política de Riesgos, que es normalizada a través de la *Guía Gestión de Riesgos y Peligros,* encontrando en el capítulo doce (12) de la guía lo relacionado con la gestión de riesgos de seguridad de la información.

Que el ICBF, mediante Resolución No. 12068 de 2019, integró y reglamentó el Comité Institucional de Gestión y Desempeño, que tiene como propósito orientar la implementación y operación del Modelo Integrado de Planeación y Gestión en el Instituto Colombiano de Bienestar Familiar.

Que es responsabilidad del Comité Institucional de Gestión y Desempeño contenida en el numeral 15 del artículo 3° de la Resolución 12068 de 2019: *"Aprobar y apoyar la implementación de los planes de continuidad del negocio que se establezcan con el fin de mitigar los riesgos asociados a la interrupción de la operación"*, y, por tanto, es necesario adoptar las acciones pertinentes para el efecto.

Que conforme a los cambios normativos y madurez en el Sistema de Gestión de Seguridad de la información, fue necesaria la revisión y ajuste a la Política de Seguridad de la Información del Instituto, y así mismo, incluir los aspectos relacionados con la Seguridad Digital y la Continuidad de la Operación.

Que en sesión virtual 03 ordinaria, realizada el día 16 de junio de 2020, el Comité Institucional de Gestión y Desempeño aprobó la adopción de la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, ajustada a los cambios anteriormente expuestos, decisión que se encuentra contenida en la respectiva acta de esa fecha.

Que dado lo anterior, se hace necesario adoptar mediante acto administración la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación en el ICBF, las Políticas Generales de Manejo, así como definir los lineamientos para su uso y manejo.

En mérito de lo expuesto,

Por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información, y se deroga la Resolución 9674 de 2018

RESUELVE:

CAPÍTULO I.
DISPOSICIONES GENERALES.

ARTÍCULO PRIMERO. Objeto. La presente Resolución tiene como objeto adoptar la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación del Instituto Colombiano de Bienestar Familiar, las Políticas Generales de Manejo, así como definir lineamientos frente a su uso y manejo.

ARTÍCULO SEGUNDO. Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación. El ICBF protege, preserva y administra la integridad, confidencialidad, disponibilidad y autenticidad de la información, así como la seguridad digital y la gestión de la continuidad de la operación, conforme al mapa de procesos, en cumplimiento de los requisitos legales y reglamentarios. La entidad previene incidentes mediante la gestión de riesgos integrales en seguridad y privacidad de la información y seguridad digital, con la implementación de controles de seguridad físicos y digitales, orientados a la mejora continua en la gestión y el alto desempeño del Sistema de Gestión de Seguridad de la Información, con la finalidad de prestar servicios con calidad y transparencia a la primera infancia, la niñez, la adolescencia, la juventud y el bienestar de las familias y comunidades colombianas.

ARTÍCULO TERCERO. Ámbito de Aplicación. La Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación y las Políticas Generales de Manejo aplica donde el Instituto Colombiano de Bienestar Familiar - ICBF tenga presencia o desarrolle su acompañamiento a través de la recolección, procesamiento, almacenamiento, recuperación, intercambio y consulta de información, en el desarrollo de la misión institucional y cumplimiento de sus objetivos estratégicos.

ARTÍCULO CUARTO. Objetivos. La Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, tendrá los siguientes objetivos:

1. Brindar mecanismos de aseguramiento para el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información del ICBF.
2. Mitigar los incidentes de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación en el ICBF.
3. Gestionar los riesgos de seguridad y privacidad de la información, Seguridad Digital y Continuidad de la operación del ICBF.
4. Establecer los lineamientos necesarios para el manejo de la información y los recursos tecnológicos del ICBF.

CAPÍTULO II.
POLÍTICAS GENERALES DE MANEJO DE INFORMACIÓN.

ARTÍCULO QUINTO. Privacidad y Tratamiento de la Información. Para el tratamiento de la información de los niños, niñas, adolescentes, la juventud, familias y comunidades colombianas a las cuales se les presta el acompañamiento en el marco del mandato legal encargado por el

Gobierno Nacional al ICBF, así como la información de los funcionarios y y contratistas que participan en el desarrollo de las funciones de dicho mandato, el ICBF cuenta con la "*Política de Tratamiento de Datos Personales del Instituto Colombiano de Bienestar Familiar*", dando cumplimiento con lo dispuesto en la Ley 1581 de 2012, reglamentada por el Capítulo 25 del Título 2 de la Parte 2 del Libro 2 del Decreto 1074 de 2015, la Ley 1712 de 2014, reglamentada por el Capítulo 2 del Título 1 de la Parte 1 del Decreto 1081 de 2015, y las demás normas externas que los modifiquen, adicionen o complementen.

ARTÍCULO SEXTO. Política de Seguridad de los Recursos Humanos. El ICBF, a través de la Dirección de Gestión Humana, debe propender para que los funcionarios y contratistas entiendan sus responsabilidades frente a la seguridad de la información con el fin de reducir el riesgo de robo, fraude, mal uso de las instalaciones y medios, asegurando la confidencialidad, disponibilidad e integridad de la información.

PARÁGRAFO. La Dirección de Contratación deberá incluir en las minutas de los contratistas cualquiera que sea su modalidad, las cláusulas u obligaciones correspondientes al Eje de Seguridad de la Información con el fin de reducir el riesgo de robo, fraude, mal uso de las instalaciones y medios, asegurando la confidencialidad, disponibilidad e integridad de la información.

ARTÍCULO SÉPTIMO. Política de Gestión de Activos. El Instituto Colombiano de Bienestar Familiar, a través de la Dirección de Información y Tecnología, establecerá y divulgará los lineamientos específicos para la identificación, clasificación y buen uso de los activos de información, con el objetivo de garantizar su protección.

a. **Inventario de Activos:** Los activos del ICBF deben ser identificados, clasificados y controlados para garantizar su uso adecuado, protección y la recuperación ante desastres. Por tal motivo, se debe llevar el inventario de los activos de información de propiedad del ICBF, discriminado por procesos, regionales y Centros Zonales, de acuerdo con la *Guía para el Desarrollo de Inventario y Clasificación de Activos*.

   Con el objetivo de establecer los controles de seguridad físicos y digitales, las dependencias que tienen la custodia de la información generada en el marco de su función se encargarán de proteger la información, de mantener y actualizar el inventario de activos de información relacionados con sus servicios (información, software, hardware y recurso humano).

b. **Archivos de Gestión:** La Dirección Administrativa a través del grupo de gestión documental y con el acompañamiento del Eje de Seguridad de la Información, deberá implementar los controles necesarios para que los archivos de gestión cuenten con los mecanismos de seguridad, con el fin de proteger y conservar la confidencialidad, integridad y disponibilidad de la información del ICBF.

c. **Clasificación de la Información:** La clasificación de la información del ICBF está definida de conformidad con la Ley 1712 de 2014 reglamentada por el Capítulo 2 del Título 1 de la Parte 1 del Decreto 1081 de 2015, la Ley 594 de 2000 (Ley General de Archivos), el Decreto 1080 de 2015 y lo estipulado en la *Guía para el Desarrollo de Inventario y*

Clasificación de Activos del ICBF, regulada por la *Guía para la Rotulación de la Información.*

ARTÍCULO OCTAVO. Responsabilidades de los Funcionarios y Contratistas frente al uso de los Recursos Tecnológicos. Todos los funcionarios y contratistas que hagan uso de los activos de información del ICBF tienen la responsabilidad de cumplir las políticas establecidas para su uso aceptable, entendiendo que el uso no adecuado de los recursos pone en riesgo la continuidad de la operación y por ende el cumplimento de la misión institucional.

a. **Del Uso del Correo Electrónico:** El servicio de correo electrónico institucional es una herramienta de apoyo a las funciones y responsabilidades de los funcionarios y contratistas del ICBF, con los siguientes lineamientos:

- El servicio de correo electrónico institucional debe ser empleado únicamente para enviar y recibir mensajes de carácter institucional. En consecuencia, no puede ser utilizado con fines personales, económicos, comerciales y/o cualquier otro ajeno a los propósitos de la Entidad.
- En cumplimiento de la iniciativa institucional del uso aceptable del papel y la eficiencia administrativa, se debe preferir el uso del correo electrónico al envío de documentos físicos, siempre que la Ley lo permita.
- Los mensajes de correo están respaldados por la Ley 527 de 1999 (por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.), la cual establece la legalidad de los mensajes de datos y las implicaciones legales que conlleva el mal uso de estos.
- La Dirección de Información y Tecnología deberá implementar herramientas tecnológicas que prevengan la pérdida o fuga de información de carácter reservada o clasificada.
- Está prohibido el envío de correos masivos (más de 150 destinatarios) a nivel nacional tanto internos como externos, salvo a través de la Dirección General, Subdirección General, Secretaría General, Oficina Asesora de Comunicaciones, Dirección de Planeación y Gestión de Control, Dirección de Gestión Humana y Dirección de Información y Tecnología.
- En las sedes regionales está prohibido el envío de correos masivos (más de 20 destinatarios) tanto internos como externos, salvo a través de los Directores Regionales, así como Coordinadores Regionales y de Centro Zonal o quien haga las veces de la Oficina Asesora de Comunicaciones.
- Para apoyar la gestión de correo electrónico de directores, subdirectores, jefes de oficina o coordinadores se debe solicitar a la mesa de servicios la delegación del buzón correspondiente, relacionando los funcionarios o contratistas que podrán escribir o responder *en nombre del* directivo con el fin de mitigar la suplantación.
- Todo mensaje sospechoso respecto de su remitente o contenido, debe ser inmediatamente reportado a la Dirección de Información y Tecnología a través de la Mesa de Servicios como incidente de seguridad según procedimiento establecido y proceder de acuerdo a las indicaciones de dicha Dirección; lo anterior, debido a que puede ser contentivo de virus, en especial si contiene archivos adjuntos con extensiones .exe, .bat,

.prg, .bak, .pif, o tenga explícitas referencias no relacionadas con la misión de la Entidad (como por ejemplo: contenidos eróticos, alusiones a personajes famosos).

- La cuenta de correo institucional no debe ser revelada en páginas o sitios publicitarios, de comercio electrónico, deportivos, agencias matrimoniales, casinos, o cualquier otra ajena a los fines de la Entidad.
- Está expresamente prohibido el uso del correo para la transferencia de contenidos insultantes, ofensivos, injuriosos, obscenos, violatorios de los derechos de autor y/o que atenten contra la integridad moral de las personas o instituciones.
- Está expresamente prohibido distribuir información del ICBF, a otras entidades o ciudadanos sin la debida autorización del Director General, Directores Regionales, Subdirector General, Directores Misionales y/o Director de Planeación y Control de Gestión, previa revisión de la Oficina Asesora de Comunicaciones en caso de comunicados y la Dirección de Planeación y Control de Gestión en caso de cifras oficiales.
- El cifrado de los mensajes de correo electrónico institucional será necesario siempre que la información transmitida esté catalogada como clasificada o reservada en el inventario de activos de información o en el marco de la Ley Colombiana vigente.
- El correo electrónico institucional en sus mensajes debe contener una sentencia de confidencialidad, que será diseñada por la Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos y debe reflejarse en todos los buzones con dominio @icbf.gov.co.
- La divulgación de cifras o datos oficiales de la Entidad sólo podrá ser emitida desde las direcciones de correo electrónico de la Dirección General, Direcciones Regionales, Subdirección General, Oficina Asesora de Comunicaciones y la Dirección de Planeación y Control de Gestión.
- Está expresamente prohibido distribuir, copiar, reenviar información del ICBF a través de correos personales o sitios web diferentes a los autorizados en el marco de sus funciones u obligaciones contractuales.
- El único servicio de correo electrónico autorizado para el manejo o transmisión de la información institucional en la Entidad es el asignado por la Dirección de Información y Tecnología, y que cuenta con el dominio @icbf.gov.co, el cual cumple con todos los requerimientos técnicos y de seguridad, evitando ataques de virus, spyware y otro tipo de software malicioso.

El ICBF se reserva el derecho de monitorear los accesos y el uso de los buzones de correo institucionales, de todos sus funcionarios o contratistas, además podrá realizar copias de seguridad en cualquier momento sin previo aviso, así como limitar el acceso temporal o definitivo, por solicitud expresa del nominador, ordenador del gasto, supervisor del contrato, jefe inmediato, Director General, Jefe de Oficina de Control Interno Disciplinario o Director de Gestión Humana a la Dirección de Información y Tecnología, así como a todos los servicios y accesos a sistemas de información de la Entidad o de terceros operados en la Entidad.

b. **Del Uso de Internet:** La Dirección de Información y Tecnología, a través del Eje de Seguridad de la Información, establecerá políticas de navegación basadas en categorías y niveles de usuario por jerarquía y funciones, las cuales deberán ser implementadas por la Subdirección de Recursos Tecnológicos, además, será responsabilidad de los funcionarios y contratistas entre otras las siguientes:

- El uso del servicio de Internet está limitado exclusivamente para propósitos laborales, contractuales e institucionales.
- Los servicios a los que un determinado usuario pueda acceder en internet dependerán del rol, obligaciones contractuales o funciones que desempeña en el ICBF y para las cuales esté formal y expresamente autorizado.
- Todo usuario es responsable de informar a la Dirección de Información y Tecnología a través de la Mesa de Servicios, los contenidos o acceso a servicios que no le estén autorizados y/o no correspondan a sus funciones u obligaciones dentro del ICBF.
- Está expresamente prohibido el envío, descarga y visualización de páginas con contenido insultante, ofensivo, injurioso, obsceno, violatorio de los derechos de autor y/o que atenten contra la integridad moral de las personas o instituciones.
- Está expresamente prohibido el acceso a páginas web, portales, sitios web y aplicaciones web que no hayan sido autorizadas por el ICBF a través de la política de navegación.
- Está expresamente prohibido el envío y descarga de cualquier tipo de software o archivos de fuentes externas, y de procedencia desconocida.
- Está expresamente prohibida la propagación de virus o cualquier tipo de código malicioso.

El ICBF se reserva el derecho de monitorear los accesos, y el uso del servicio de internet de todos sus funcionarios o contratistas, además de limitar el acceso a determinadas páginas de Internet, los horarios de conexión, los servicios ofrecidos por la red, la descarga de archivos y cualquier otro ajeno a los fines de la Entidad.

c. **Del Uso de los Recursos Tecnológicos:** Los recursos tecnológicos del ICBF son herramientas de apoyo a las labores, obligaciones y responsabilidades de los funcionarios y contratistas. Por ello, su uso está sujeto a las siguientes directrices:

    - Los bienes de cómputo se emplearán de manera exclusiva y bajo la completa responsabilidad por el funcionario o contratista al cual han sido asignados, únicamente para el desempeño de las funciones del cargo o las obligaciones contractuales pactadas. Por tanto, no pueden ser utilizados con fines personales o por terceros no autorizados por la Dirección de Información y Tecnología mediante solicitud formal de los Directores, Subdirectores, Jefes de Oficina o Coordinadores de Grupos del ICBF a través de la Mesa de Servicios.
    - Sólo está permitido el uso de software licenciado por la Entidad y/o aquel que, sin requerir licencia, sea expresamente autorizado por la Dirección de Información y Tecnología a través de la Subdirección de Recursos tecnológicos. Las aplicaciones generadas o adquiridas por el ICBF en desarrollo de su operación institucional y que no fueron desarrollados por el ICBF deben ser reportadas a la Dirección de Información y Tecnología a través de la Subdirección de Sistemas Integrados de Información, para su administración.
    - En caso de que el colaborador deba hacer uso de equipos ajenos al ICBF, estos deberán cumplir con la legalidad del Software instalado, antivirus licenciado, actualizado y solo podrá conectarse a la red del ICBF una vez esté avalado por los ingenieros de la Subdirección de Recursos Tecnológicos a nivel Central e Ingenieros Regionales en el nivel Regional y Zonal. La Subdirección de Recursos

Tecnológicos deberá realizar la revisión de los requisitos antes mencionados de manera periódica en los equipos autorizados para conectarse a la red de ICBF.

- Es responsabilidad de los funcionarios y contratistas mantener copias de seguridad de la información contenida en sus estaciones de trabajo y entregarlas al ICBF en custodia al finalizar la vinculación con la Entidad.
- Los usuarios no deben mantener almacenados en los discos duros de computadores de escritorio, portátiles o discos virtuales de red, archivos de video, música y fotos que no sean de carácter institucional o que atenten con los derechos de autor o propiedad intelectual de los mismos.
- No está permitido fumar, ingerir alimentos o bebidas en el área de trabajo donde se encuentren elementos tecnológicos o información física que pueda estar expuesta a su daño parcial o total y, por ende, a la pérdida de la integridad de esta.
- No está permitido realizar conexiones o derivaciones eléctricas que pongan en riesgo los elementos tecnológicos por fallas en el suministro eléctrico a los equipos de cómputo, salvo en aquellos casos que sean autorizados por la Dirección Administrativa o quien haga sus veces en el nivel Regional o Zonal.
- Las únicas personas autorizadas para hacer modificaciones o actualizaciones en los elementos y recursos tecnológicos, como destapar, agregar, desconectar, retirar, revisar y/o reparar sus componentes, son los designados por la Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos para tal labor.
- La Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos realizará monitoreo sobre los dispositivos de almacenamientos externos como USB, CD-ROM, DVD, Discos Duros externos, entre otros, con el fin de prevenir o detectar fuga de información.
- La única dependencia autorizada para trasladar los elementos y recursos tecnológicos de un puesto a otro será la Dirección de Información y Tecnología o quien haga sus veces en el nivel regional y zonal, sin embargo, desde y hacia el almacén será la Dirección Administrativa o quien haga sus veces en el nivel regional y zonal, con el fin de llevar el control individual de inventarios. En tal virtud, toda reasignación de equipos deberá ajustarse a los procedimientos y competencias de la gestión de bienes de la Entidad.
- La pérdida o daño de elementos o recursos tecnológicos, o de alguno de sus componentes, deberá ser informada de inmediato a la Dirección Administrativa por el funcionario o contratista a quien se le hubiere asignado.
- La pérdida de información deberá ser informada con detalle a la Dirección de Información y Tecnología a través de la Mesa de Servicios como incidente de seguridad.
- Todo incidente de seguridad que comprometa la disponibilidad, integridad o confidencialidad de la información física o digital deberá ser reportado a la mayor brevedad posible a través de la Mesa de Servicios, siguiendo el procedimiento establecido.
- La Dirección de Información y Tecnología es la única dependencia autorizada para la administración del software, el cual no deberá ser copiado, suministrado a terceros ni utilizado para fines personales.

- Todo acceso a la red de la Entidad mediante elementos o recursos tecnológicos no institucionales deberá ser informado, autorizado y controlado por la Dirección de Información y Tecnología a través de la Subdirección de Recursos Tecnológicos.
- La conexión a la red wifi institucional para funcionarios deberá ser administrada desde la Dirección de Información y Tecnología mediante un SSID (Service Set Identifier) único a nivel nacional, la autenticación deberá ser con usuario y contraseña de directorio activo.
- La conexión a la red institucional para visitantes deberá tener un SSID y contraseñas diferentes para cada sede administrativa (Sede de la Dirección General, Regional y Zonal), administrada por la Dirección de Información y Tecnología o quien haga sus veces en el nivel Regional y Zonal; la contraseña deberá cambiar diariamente y solo estará disponible en el horario laboral definido en la resolución de horario de cada sede.
- No se podrá conectar dispositivos celulares personales a la red wifi de funcionarios, salvo los de la Oficina Asesora de Comunicaciones, Dirección General y los aprobados por la Dirección de Información y Tecnología o quien haga sus veces en las sedes Regionales y Zonales a través de una solicitud por módulo de autoservicio en la herramienta de mesa de servicios.
- Los equipos deben quedar apagados cada vez que el funcionario o contratista no se encuentre en la oficina o durante la noche, esto, con el fin de proteger la seguridad y distribuir bien los recursos de la Entidad, siempre y cuando no vaya a realizar actividades vía remota.
- Todo dispositivo móvil institucional, que transmita y/o almacene información sensible de la Entidad, debe ser monitoreado a través de la herramienta de gestión tecnológica definida por la Dirección de Información y Tecnología.
- Todo dispositivo móvil personal que requiera acceder a los servicios tecnológicos de la Entidad, y que trasmita y/o almacene información sensible, debe ser monitoreado a través de la herramienta tecnológica definida por la Dirección de Información y Tecnología.

d. **Del Uso de los Sistemas o Herramientas de Información:** Todos los funcionarios y contratistas del ICBF son responsables de la protección de la información que acceden y/o procesan, así como de evitar su pérdida, alteración, destrucción y uso indebido, para lo cual se dictan los siguientes lineamientos:

- Las credenciales de acceso a la red y a los recursos informáticos (Usuario y Clave) son de carácter estrictamente personal e intransferible; los funcionarios y contratistas no deben revelarlas a terceros ni utilizar claves ajenas.
- Todo funcionario y contratista es responsable del cambio de clave de acceso a los sistemas de información o recursos informáticos periódicamente.
- Todo funcionario y contratista es responsable de los registros y modificaciones de información que se hagan a nombre de su cuenta de usuario.
- En ausencia del funcionario o contratista, el acceso a la estación de trabajo le será bloqueada con una solicitud a la Dirección de Información y Tecnología a través de la Mesa de Servicios, con el fin de evitar la exposición de la información y el

acceso a terceros, que puedan generar daño, alteración o uso indebido, así como a la suplantación de identidad. La Dirección de Gestión Humana debe reportar cualquier tipo de novedad de los funcionarios y el Supervisor del Contrato las novedades de los contratistas.

- Cuando un funcionario o contratista cesa en sus funciones o culmina la ejecución de contrato del ICBF, todos los privilegios sobre los recursos informáticos otorgados le serán suspendidos inmediatamente; la información del empleado y/o contratista serán almacenados en un repositorio de los servidores de la Entidad.
- Cuando un funcionario o contratista cesa en sus funciones o culmina la ejecución de contrato del ICBF, el supervisor o jefe inmediato es el encargado de la custodia de los recursos de información, incluyendo la cesión de derechos de propiedad intelectual de acuerdo con la normativa vigente.
- Todos los funcionarios y contratistas de la Entidad deben dar estricto cumplimiento a lo estipulado en la Ley 23 de 1982 "Sobre derechos de autor", la Decisión 351 de 1993 de la Comunidad Andina de Naciones, así como cualquier otra que adicione, modifique o reglamente la materia.

ARTÍCULO NOVENO. Política de Control de Acceso. Los propietarios de los activos de información deben establecer medidas de control de acceso a nivel de red, sistema operativo, sistemas de información, servicios de tecnologías de la información e infraestructura física, con el fin de mitigar riesgos asociados al acceso a la información y servicios de infraestructura tecnológica de personal no autorizado, salvaguardando la integridad, disponibilidad y confidencialidad de la información del ICBF.

ARTÍCULO DÉCIMO. Política de Criptografía. La Dirección de Información y Tecnología deberá contar con controles en el uso adecuado y efectivo de la criptografía para proteger la confidencialidad, integridad y disponibilidad de la información.

ARTÍCULO DÉCIMO PRIMERO. Política de Seguridad Física y del Entorno. El ICBF debe contar con controles para la protección del perímetro de seguridad de las instalaciones físicas, controlar el acceso del personal y la permanencia en las oficinas e instalaciones, así como controlar el acceso a áreas restringidas (áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones), además mitigar los riesgos y amenazas externas y ambientales, con el fin de evitar afectación a la confidencialidad, disponibilidad e integridad de la información de la Entidad.

PARÁGRAFO 1. Todos los funcionarios, contratistas y visitantes que se encuentren en las instalaciones físicas del ICBF deben estar debidamente identificados, con un documento que acredite su tipo de vinculación, el cual deberá portarse en un lugar visible.

PARÁGRAFO 2. Los visitantes en el ICBF siempre deben permanecer acompañados por un funcionario o contratista debidamente identificado.

PARÁGRAFO 3. El personal de empresas contratistas que desempeñen funciones de forma permanente en las instalaciones del ICBF, debe estar identificado con carné y chalecos o distintivos del Contratista y portar el carné de la ARL.

ARTÍCULO DÉCIMO SEGUNDO. Política de Seguridad de las Operaciones. La Dirección de Información y Tecnología, a través de la Subdirección de Recursos Tecnológicos, será la encargada de la operación y administración de los recursos tecnológicos que soportan la operación del ICBF. Así mismo, velará por la eficiencia de los controles asociados a los recursos tecnológicos protegiendo la confidencialidad, integridad y disponibilidad de la información, así como la de asegurar que los cambios efectuados sobre los recursos tecnológicos, serán controlados y debidamente autorizados. De igual manera, deberá proveer la capacidad de procesamiento requerida en los recursos tecnológicos y los sistemas de información del ICBF, efectuando proyecciones de crecimiento y provisiones en la plataforma tecnológica de acuerdo con el crecimiento de la Entidad.

La Dirección de Información y Tecnología, a través de la Subdirección de Recursos Tecnológicos, deberá realizar y mantener copias de seguridad de la información de la Entidad en medio digital, siempre que ésta sea reportada por el responsable de la misma, con el objetivo de recuperarla en caso de cualquier tipo de falla, ya sea de hardware, software, o de procedimientos operativos al interior de la Entidad.

Se efectuará la copia respectiva de acuerdo con el esquema definido previamente en el documento Procedimiento Gestión Copias de Seguridad de la Entidad, el cual deberá ser diseñado por la Subdirección de Recursos Tecnológicos, en conjunto con los líderes de Proceso.

ARTÍCULO DÉCIMO TERCERO. Política de Seguridad de las Comunicaciones. La Dirección de Información y Tecnología, a través de la Subdirección de Recursos Tecnológicos, establecerá los mecanismos necesarios para proveer la disponibilidad de las redes y de los servicios que dependen de ellas, así mismo, dispondrá y monitoreará los mecanismos necesarios de seguridad para proteger la integridad y la confidencialidad de la información del ICBF.

PARÁGRAFO 1. Como parte de sus términos y condiciones iniciales de trabajo, los funcionarios o contratistas, cualquiera sea su nivel jerárquico dentro de la entidad, firmarán un Compromiso de Confidencialidad y no divulgación, en lo que respecta al tratamiento de la información de la Entidad, y de igual manera la Autorización de tratamiento de datos personales, en los términos de la Ley 1581 de 2012, así como el capítulo 25 del Decreto 1074 de 2015 y la Ley 1712 de 2014 reglamentada por el capítulo 2 del Decreto 1081 de 2015 y las demás normas que las adicionen, modifiquen, reglamenten o complementen. Dicho compromiso y autorización (documento original) deberá ser retenido en forma segura por la Dirección de Gestión Humana (funcionarios), la Dirección de Contratación (contratistas) o quien haga las veces en las Direcciones Regionales, según el caso. Así mismo, mediante el Compromiso de Confidencialidad el funcionario o el contratista declarará conocer y aceptar la existencia de determinadas actividades que pueden ser objeto de control y monitoreo. Estas actividades deben ser detalladas a fin de no violar el derecho a la privacidad ni los derechos del funcionario o contratista.

PARÁGRAFO 2. Para el caso del personal que ejecute tareas propias del ICBF y haya sido contratado en el marco de un contrato o convenio con el ICBF, debe reposar en la carpeta de

ejecución del contrato un compromiso de confidencialidad debidamente suscrito por el Representante Legal de la empresa contratista o con la cual se realiza el convenio.

ARTÍCULO DÉCIMO CUARTO. Política de Seguridad para la Adquisición, Desarrollo y Mantenimiento de Sistemas. La Dirección de Información y Tecnología, a través de la Subdirección de Sistemas Integrados de Información, velará porque el desarrollo interno o externo de los sistemas de información cumpla con los requerimientos de seguridad adecuados para la protección de la información del ICBF.

La Dirección de Información y Tecnología será la única dependencia de la Entidad con la capacidad de adquirir, desarrollar o avalar la adquisición y recepción de software de cualquier tipo, conforme a los requerimientos de las diferentes dependencias, con el fin de garantizar la conveniencia, soporte, mantenimiento y seguridad de la información de los sistemas que operan en el Instituto.

En consecuencia, cualquier software que opere en el Instituto y no haya sido entregado a la Dirección de Información y Tecnología, no serán responsabilidad de la misma, no se le brindará soporte y no se le salvaguardará la información.

ARTÍCULO DÉCIMO QUINTO. Política de Seguridad para Relación con Proveedores. El ICBF establecerá mecanismos de control en relaciones con sus proveedores, teniendo en cuenta que se debe asegurar la información a la que tengan acceso, supervisando el cumplimiento de lo establecido en el Eje de seguridad de la información. Los Supervisores de los contratos o convenios en conjunto con la Dirección de Información y Tecnología, tendrán la responsabilidad de la divulgación y revisión del cumplimiento de las políticas y procedimientos de la seguridad de la información.

ARTÍCULO DÉCIMO SEXTO. Política de Gestión de Incidentes de Seguridad de la Información. El ICBF promoverá entre los funcionarios y contratistas el reporte de incidentes relacionados con la seguridad de la información y sus medios, reporte y seguimiento. Así mismo, asignará responsables para el tratamiento de los incidentes de seguridad de la información, quienes tendrán la responsabilidad de investigar y solucionar los incidentes reportados, de acuerdo con su criticidad. El Director General o a quien éste delegue, son los únicos autorizados para reportar incidentes de seguridad ante las autoridades; así mismo, son los únicos canales de comunicación autorizados para hacer pronunciamientos oficiales ante entidades externas, medios de comunicación o la ciudadanía.

ARTÍCULO DÉCIMO SÉPTIMO. Política de la Continuidad de la Operación. El ICBF dispondrá los planes necesarios para la implementación del proceso de continuidad de la operación de los servicios, los cuales serán operados por los líderes de los procesos del modelo de operación. La Secretaría General liderará la elaboración del Análisis de Impacto al Negocio (BIA) y del Plan de Continuidad de los Servicios, así como la activación de este cuando sea necesario.

ARTÍCULO DÉCIMO OCTAVO. Política de Cumplimiento. El ICBF velará por la identificación, documentación y cumplimiento de los requisitos legales enmarcados en la seguridad de la información del Estado colombiano, entre ella la referente a derechos de autor y propiedad

intelectual, protección de datos personales, ley de transparencia y del derecho de acceso a la información pública nacional y las consignadas en la Matriz de Requisitos Legales del ICBF.

PARÁGRAFO. El plan de continuidad de tecnologías deberá incluirse en el Plan de Continuidad de la Operación del ICBF, los Planes de Emergencia y Contingencia, así como cualquier estrategia alineada a la continuidad de la prestación del servicio de Bienestar Familiar.

ARTÍCULO DÉCIMO NOVENO. Lineamientos de las Políticas de Seguridad de la Información. Todas las políticas contenidas en el Capítulo II de este acto administrativo se encuentran reglamentadas en los documentos, Declaración de Aplicabilidad y Manual de Política de Seguridad de la Información, los cuales están anexos al Manual del Sistema Integrado de Gestión del ICBF, aprobado mediante Resolución 8080 de 2016 y son parte integral de este documento.

CAPÍTULO III.
REVISIÓN, VIGENCIA Y DEROGATORIA.

ARTÍCULO VIGÉSIMO. Revisión. La Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, será revisada anualmente, o antes si existiesen modificaciones que así lo requieran, para que se mantenga oportuna, suficiente y eficaz. Este proceso será liderado por la Dirección de Información y Tecnología, y revisados por el Comité Institucional de Gestión y Desempeño.

ARTÍCULO VIGÉSIMO PRIMERO. Vigencia y Derogatoria. La presente Resolución rige a partir de la fecha de su publicación, deroga la Resolución No. 9674 de 2018, así como todas aquellas disposiciones que le sean contrarias.

PUBLÍQUESE, COMUNÍQUESE Y CÚMPLASE 27 JUL 2020
Dada en Bogotá, D.C., a los

LINA ARBELÁEZ ARBELÁEZ
Directora General

Aprobó: Alvaro A. Rueda Zapata ___ - Director de Información y Tecnología / Amanda Castellanos Mendoza ___ - Directora de Planeación y Control de Gestión / Édgar Leonardo Bojacá Castro ___ - Jefe Oficina Asesora Jurídica
Revisó: Daniel E. Lozano / Mónica Nieto ___ – Oficina Asesora Jurídica / Asesor (a)– ___ - Dirección General
Elaboró: Dayana Carbonó Carbonó ___ – Dirección de Información y Tecnología